IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	**CRIMINAL ACTION**
v.	:	
	:	**NO. 20-421-1**
GEOFFREY HINES	:	

MEMORANDUM OPINION

Goldberg, J. **June 14, 2022**

Following a warrant-based search of his digital devices, Defendant Geoffrey Hines was charged with fourteen counts of using an interstate commerce facility to entice a minor to engage in sexually explicit conduct (18 U.S.C. § 2422(b)), fourteen counts of manufacturing and attempted manufacturing of child pornography (18 U.S.C. § 2251(a), (e)), and one count of possession of child pornography (18 U.S.C. § 2252(a)(4)(B), (b)(2)). Defendant now moves to suppress the evidence seized pursuant to the search warrant. He also seeks to suppress incriminating statements he made both while the search warrant was being executed and after he was arrested on grounds that they are tainted by the defective warrant. For the following reasons, I will deny Defendant's Motion.

I. FACTUAL BACKGROUND

A. The Search Warrant Affidavit

On May 18, 2020, Detective Sergeant Kenneth Bellis of the Delaware County Criminal Investigation Division ("CID") prepared a twenty-six page affidavit of probable cause in support of a search warrant for all digital devices at the "Subject Residence" at 7245 Clinton Road, Upper Darby, Delaware County, Pennsylvania The affidavit included the following facts:

- Sergeant Bellis is a member of a federal Task Force that directs its efforts in the area of Internet Crimes Against Children ("ICAC") and had been a law enforcement officer for approximately 29 years. He was assigned to and sworn as a Task Force Officer with the FBI, and conducted and participated in numerous investigations regarding child exploitation

on the Internet. (Def.'s Mot. to Suppress, Ex. A, Affidavit in Support of Search Warrant ("Affidavit") ¶¶ 1–4.)

- In July 2019, the National Center for Missing and Exploited Children began receiving numerous reports from the video live streaming service "Twitch" Interactive. Twitch primarily focuses on video game live streaming and can be accessed from almost every platform where people watch video. The service allows users to capture moments from live broadcasts and videos on demand ("VOD") through a process entitled "clipping." Once the clip is prepared, it can then be shared with other users. (Id. ¶¶ 12–15.)

- A suspect target using the internet services at 7245 Clinton Road, Upper Darby, Pennsylvania offered to make "donations" or pay "v-bucks" to child victims if they would remove their clothes and engage in sexually explicit conduct via live stream with the target. V-bucks are a form of in-game currency used in the game Fortnight. (Id. ¶¶ 16–18.)

- Twitch reported more than fifty users who they identified as suspected users who were asked to expose their genitalia and send sexually explicit content to the target user. The sexually exploitative chats with each child victim were each similar in nature, but different user names and email addresses were used to communicate with these suspected children. Nevertheless, Twitch identified the majority of the communications as coming from just two IP addresses, both of which resolved back to 7245 Clinton Road, Upper Darby, Pennsylvania. Other IP addresses associated with the target of the investigation were believed to have been accessed through a proxy server, which is a server application that serves as an intermediary between the user requesting the information and the destination, potentially masking the true origin or identity of the requestor. (Id. ¶¶ 19–20.)

- As part of the Cypertips, Twitch provided the content of the communications and video capture between the target accounts and the suspected child victims to law enforcement. (Id. ¶ 21.)

- One such communication on June 12, 2019 in which the target entered a Twitch chat room with a minor boy approximately nine to eleven years old. The target offered the minor 3000 v-bucks to take off his pajamas and underwear and show his genitalia. The boy did so. Law enforcement identified the child as being a nine-year old in the United Kingdom (Id. ¶¶ 22–24.)

- Another communication occurred on June 16, 2019, when the target entered a Twitch chat room and communicated with a user later confirmed to be a twelve-year old boy. Again, the target offered the boy v-bucks in exchange for video of his genitalia. Although the boy went into the bathroom, he did not pull down his pants for the target. (Id. ¶ ¶ 25–28.)

- A third communication with a child user occurred on June 30, 2019, during which the target communicated with the suspected child during a video game live stream and sent a stream of messages to the child, asking the child to remove his shorts and inquiring whether the child could "cum yet." (Id. ¶ 29.)

- Also on June 30, 2019, the subject communicated with the suspected child during a video game live stream and offered him v-bucks to "jerk off" over the live stream. (Id. ¶ 30.)

- The affidavit details similar types of communications from the target user with minor victims occurring on July 3, 2019, July 7, 2019 (two communications), January 20, 2020 (three communications), and February 17, 2020. These communications were verified through review of the live stream videos and/or interviews with the victims and their families. In addition, investigators issued two administrative subpoenas for the IP addresses used in the communications, which identified the subscriber to both IP addresses as Rose Morgan at 7245 Clinton Road, Upper Darby, Pennsylvania. (Id. ¶ 31–47.)

- Based upon these facts, Sergeant Bellis represented that there was probable cause to believe that a user of computer devices located at 7245 Clinton Road, Upper Darby, Pennsylvania was responsible for the above communications. He averred that, based on his experience, it was likely that the child pornography files had been transferred from one device to another and one account to another. (Id. ¶¶ 52–54.)

The warrant face sheet identified the items to be searched and seized, and it incorporated the application and affidavit, as follows:

ATTACHMENT "A"

The below items will be searched for evidence of violations of Pennsylvania Crimes Code Title 18, Section §6312 - Sexual Abuse of Children, Title 18, Section §7512 – Criminal use of a communication facility.

The items to be seized and manner of search are in keeping with the dictates as set forth in Commonwealth v. Green, 204 A.3rd 469, 480-482 (Pa Super. 2019) Said items have been described as specifically as is reasonably possible and the seized devices will be searched only for evidence related to the referenced criminal offenses.

1. All child pornographic images, including digital evidence contained on the electronic devices or storage media seized as a result of this search and seizure warrant. All visual depictions of minors engaged in sexually explicit conduct produced using minors engaged in such conduct, including those in opened or unopened emails or text messages. These include both originals and copies.

2. All documents, to include in electronic form, and stored communications including contact information, text messages, call logs, voicemails, Internet searches, Internet history, photographs, and any other electronic data or other memory features contained in the devices, smart phones, cell phones, computers, or SIM cards including correspondence, records, opened or unopened emails, text messages, chat logs, pertaining to the possession, receipt, access to or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Pennsylvania Crimes Code Title 18, Section 6312 (Sexual Abuse of Children), or pertaining to an interest in child pornography or minors whether transmitted or received, or which tends to show the knowing manufacturing and possession of any child pornography possessed.

3. All computer hardware, including but not limited to any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Any computer processing units, internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives, and diskettes, tape drives, tapes, flash drives, and optical storage devices), peripheral input / output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers), and related communication devices (such as modems, cables, and connections), recording equipment, as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware. Any electronic devices, including but not limited to cellular telephones, gaming devices, MP3 players, and e-readers. These items will be seized and then later searched for evidence relating to the possession and / or distribution of child pornography.

4. All communications and files associated with minor victims involving sexual topics or in an effort to harass minor victims, threaten minor victims, seduce a minor, meet a minor, or manufacture child pornography.

ATTACHMENT "A" Continued

5. All records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP), cell phone service provider, or electronic service provider, relating to the ownership or use of the computer equipment or electronic devices seized. Any documents that show ownership or who resides at the place to be searched.

6. SOFTWARE: Software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word processing, graphics, or spread sheet programs), utilities, compilers, and communications programs. These items will be seized in order to facilitate the search of the computer systems / computer system components / computer system storage media named above. The reason for these items to be seized are outlined in the affidavit of this search warrant and incorporated herein by reference.

7. DOCUMENTATION: Computer related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items. These items will be seized in order to facilitate the search of the computer systems / computer system components / computer system storage media named above. The reason for these items to be seized are outlined in the affidavit of this search warrant and incorporated herein by reference.

8. PASSWORDS AND DATA SECURITY DEVICES: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming codes. A password (string of alpha-numeric characters) usually operates as a sort of digital key to unlock particular data security devices. These items will be seized in order to facilitate the search of the computer systems / computer system components / computer system storage media named above. Documents of any nature, printed or hand written, which may relate to passwords that will assist in searching devices seized. The reason for these items to be seized are outlined in the affidavit of this search warrant and incorporated herein by reference.

9. Transaction records, including V-Bucks transactions, gift card purchases, PayPal records, bank records, credit card records, used to make donations to a child victim found in the suspect residence, or on equipment seized from the suspect residence. V-bucks are a form of in-game currency used in the game Fortnight. V-bucks can be transferred to a user through the purchase of a gift card depending on the system being used (See affidavit paragraph numbers 16-18)

Sergeant Bellis noted that, in keeping with the dictates set forth in Commonwealth v. Green, 204 A.3d 469, 480–82 (Pa. Super. Ct. 2019), the seized devices would be searched "only for evidence related to the referenced criminal offenses." (Id. at Attachment A.)

Based on this affidavit, the search warrant was issued for 7245 Clinton Road, Upper Darby, Pennsylvania to search and seize all child pornographic images, all documents, all computer hardware, all records, documents, invoices, notes, and materials that pertain to accounts with any internet service provider, cell service provider, or electronic service provider. (Id.)

B. Other Relevant Facts

The parties agree to the following facts:

On May 19, 2020, the search warrant was executed by detectives from the Delaware County District Attorney's Office Criminal Investigation Division, Pennsylvania Internet Crimes Against Children Taskforce, and Upper Darby Police. Detectives seized several electronic devices including (1) a custom-built desktop computer, (2) a Toshiba external storage drive, (3) a Hewlett Packard laptop computer, (4) two SanDisk Cruzer flash drives, (5) cellular telephones, and (6) a Sony PlayStation. Detectives also recovered gift cards that appeared to have been redeemed.

Defendant was home when investigators executed the search warrant, and he agreed to speak privately to Sergeant Bellis and Detective Pisani on location at 8:00 a.m. Sergeant Bellis advised Defendant that he was not under arrest, was not in police custody, and did not have to speak to them. During the ensuing conversation, which was recorded, Defendant made incriminating statements regarding his communications with minors on Twitch, confessing that he created numerous user accounts on Twitch to communicate with minor boys and enticed them to commit sexually explicit acts. Defendant was then placed under arrest and agreed to another interview with Bellis and Pisani while in custody at police headquarters at 12:41 p.m. Defendant was read his Miranda rights and signed a Miranda waiver. During that interview, Defendant made additional incriminating statements about his involvement with child pornography and also confessed to sexually abusing his family member when that child was six years old. When questioned further about the sexual abuse, Defendant terminated the interview, and all communication was ceased by law enforcement.

A forensic examination of the computer devices seized from Defendant's home revealed more than twenty-five videos of minor children exposing their genitalia and 1,000 videos of solicitation, with a number of those videos depicting children complying with the solicitation. The forensic examination also revealed an extensive collection of more than 47,000 images of child pornography, many of which were manufactured by Defendant. Most of the images depicted young boys being sexually abused, and many involved sexually sadistic abuse. The videos dated as far back as 2015 and extended all the way to April of 2020.

II. STANDARD OF REVIEW

When reviewing a magistrate judge's determination of probable cause to issue a warrant, a district court should "[pay] great deference" to the magistrate's decision. Illinois v. Gates, 462 U.S. 213, 236 (1983). This standard means that "the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants." United States v. Ventresca, 380 U.S. 102, 109 (1965). If a substantial basis exists to support the probable cause finding, the court must uphold that finding even if it or a "different magistrate judge might have found the affidavit insufficient to support a warrant." United States v. Conley, 4 F.3d 1200, 1205 (3d Cir. 1993) (quoting United States v. Jones, 994 F.2d 1051, 1057 (3d Cir. 1993)).

Such deference, however, "does not mean that reviewing courts should simply rubber stamp a magistrate's conclusions." United States v. Tehfe, 722 F.2d 1114, 1117 (3d Cir. 1983). Rather, the duty of the reviewing court is to "ensure that the state district justice had a 'substantial basis' for concluding that the affidavit supporting the warrant established probable cause." United States v. Mortimer, 387 F. App'x 138, 140 (3d Cir. 2005) (citing Jones, 994 F.2d at 1054); see also Conley, 4 F.3d at 1205 ("Keeping in mind that the task of the issuing magistrate is simply to determine whether there is a fair probability that contraband or evidence of a crime will be found in a particular place, a reviewing court is to uphold the warrant as long as there is a substantial basis for a fair probability that evidence will be found.") (internal quotation marks omitted).

III. DISCUSSION

Defendant moves to suppress the evidence seized pursuant to the search warrant. He claims that the warrant failed to meet the Fourth Amendment's particularity requirement because it did not state with particularity the items to be searched or seized, thus allowing the government to "rummage" around in Defendant's personal effects. In addition, as noted above, he contends that the incriminating statements he gave to police were derived from the initial unlawful search and must also be suppressed.

A. Whether the Search Warrant Was Sufficiently Particular

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizure, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized.*

U.S. Const. amend. IV (emphasis added).

The particularity requirement—"the touchstone of [the] warrant," Doe v. Groody, 361 F.3d 232, 239 (3d Cir. 2004)—is satisfied by expressly listing items to be seized or expressly incorporating by reference an affidavit that lists such items. See Bartholomew v. Pennsylvania, 221 F.3d 425, 428–29 (3d Cir. 2000) (holding that if a warrant's particularity depends upon incorporated documents, those documents must physically accompany the warrant). The requirement that the warrant particularly describe—rather than imply or assume—the items to be seized is critical to serving one of the Fourth Amendment's key purposes: "to limit the [searching] agents' discretion as to what they are entitled to seize" and "to inform the subject of the search what can be seized." Id. at 429; see also United States v. Wright, 493 F. App'x 265, 268 (3d Cir. 2012) (quoting Bartholomew).

As such, the United States Court of Appeals for the Third Circuit has imposed two requirements upon warrants that seek to satisfy the particularity requirement through incorporation by reference to an affidavit. First, "the warrant must expressly incorporate the affidavit, and the incorporation must be clear." United States v. Tracey, 597 F.3d 140, 147 (3d Cir. 2010) (internal quotation omitted). Second, the affidavit must accompany the warrant; it cannot be impounded and sealed. See Bartholomew, 221 F.3d at 429–430 ("[W]here the list of items to be seized does not appear on the face of the warrant, sealing that list, even though it is 'incorporated' in the warrant, would violate the Fourth Amendment."). "Ultimately, the particularity requirement intends that 'nothing is left to the discretion of the officer executing the warrant.'" United States v. Perez, 712 F. App'x 136, 139 (3d Cir.

2017) (quoting Marron v. United States, 275 U.S. 192, 196 (1927)). A warrant need not be technically perfect, however, as "[t]he standard . . . is one of practical accuracy rather than technical nicety." United States v. Bedford, 519 F.2d 650, 655 (3d Cir. 1975) (quotations omitted).

Here, Defendant argues that the warrant authorizing the search of his home and computer devices did not comply with the particularity requirement of the Fourth Amendment and effectively gave the executing agents unlimited discretion to "rummage" through his property. Defendant posits that although the warrant specified that the types of *data* to be searched for included child pornographic images and visual depictions of minors engaged in sexual conduct, the warrant provided "virtually no limits" on the description of items to be seized. (Def.'s Mot. 9.) For example, he notes that the warrant's description did not include specific, enumerated items to be seized, but instead simply stated the agents were to search for "all documents," "all computer hardware," "all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider (ISP)." (Id. at Ex. A.) According to Defendant, the warrant also allowed for the seizure of "software," "documentation," and "passwords and data security devices" without providing any guidance about what type of software, documentation, passwords, and data security devices agents should seize, and without limiting it to specific date or time periods. Defendant goes on to assert that this lack of specificity in the search warrant was particularly flawed because the information was available to the Government to make the description of the items to be seized much more particular. For example, according to Defendant, the Government "could have provided more particularity by using common search limitations like specific software used to download or store child pornography." (Id. at 10.) Defendant contends that because the warrant lacked the requisite particularity required by the Fourth Amendment, the warrant was improper and any evidence seized pursuant to the search must be suppressed.

I disagree with Defendant's argument on several grounds. Primarily, with respect to Defendant's contention that the search warrant face sheet failed to state with particularity the items to be searched for and seized, the United States Court of Appeals for the Third Circuit has observed that "it is perfectly

appropriate to construe a warrant in light of an accompanying affidavit or other document that is incorporated within the warrant." Groody, 361 F.3d at 239 (3d Cir. 2004). To take advantage of this principle of interpretation, however, the warrant must expressly incorporate the affidavit. Id. (citing Bartholomew, 221 F.3d at 428. "'When a warrant is accompanied by an affidavit that is incorporated by reference, the affidavit may be used in construing the scope of the warrant.'" Bartholomew, 221 F.3d at 428 (quoting United States v. Johnson, 690 F.2d 60, 64–65 (3d Cir. 1982)). The United States Supreme Court has emphasized that the warrant must use "appropriate words of incorporation" and the "supporting document [must] accompan[y] the warrant." Groh v. Ramirez, 540 U.S. 551, 558 (2004).

Here, the search warrant face sheet properly incorporated the application and affidavit contained in "Attachment A" to the search warrant. Specifically, the face sheet stated:

> IDENTIFY ITEMS TO BE SEARCHED FOR AND SEIZED (Be as specific as possible):
>
> Evidence in violation of PA Title 18 §6312 – Sexual Abuse of Children & PA Title 18 §7512 – Crimin[al] use of a communicate[o]n facility.
>
> SEE ATTACHMENT "A"

(Def.'s Mot., Ex. A.) The face sheet also specifically noted that the warrant application was a total of 26 pages, which included Attachment A. Attachment "A" itself was labeled as part of the "Application for Search Warrant – Continuation Pages" and begins at "Page 2 of 26 Pages" of the warrant application (Id.) The warrant application then listed the precise evidence subject to search and seizure, with each page being numbered with both the current page number and total number of pages in the packet to ensure no mistake as to what comprised the search warrant. Accordingly, I find that the warrant appropriately incorporated Attachment "A" and the affidavit, both of which were appended to the warrant application. [1]

[1] By contrast, in both Groh and Groody, the warrant face sheet failed to include any language incorporating the affidavit for purposes of construing the scope of the warrant. Groh, 540 U.S. at 558–60; Groody, 361 F.3d at 239.

Second, Attachment "A" provided extensive specificity in terms of the items to be searched, describing in detail categories such as images, documents, hardware, software, and passwords. Such classifications are appropriate in complex situations, as the particularity requirement "must be applied with a practical margin of flexibility." United States v. Fattah, 858 F.3d 801, 819 (3d Cir. 2017) (quotation omitted). Indeed, the Third Circuit has observed that because of individuals' ability to "hide, mislabel, or manipulate files," in cases of electronic-based crimes, there may be "no practical substitute for actually looking in many (perhaps all)" files and locations during a search of digital storage. United States v. Stabile, 633 F.3d 219, 237, 239 (3d Cir. 2011) (quotation omitted). This principle also holds true as to Defendant's objection to the lack of date limitations in the warrant. As noted in the Affidavit, Defendant's conduct occurred over the course of years, and the typical child pornography collector tends to hold on to the illicit material for many years, meaning date restrictions on the material that may be collected would be inappropriate. (Affidavit ¶¶ 11(b), 55.)

Importantly, the document limited the search and seizure to evidence of the violations of the two criminal statutes that Defendant was suspected of violating. The warrant application also provided that, in keeping with the dictates of Commonwealth v. Green, 204 A.3d 469, 480–82 (Pa. Super. 2019), the items seized would be searched only for evidence related to those criminal offenses. See Green, 204 A.3d at 481 ("[A]warrant may permit the seizure of electronic equipment so long as the search of the equipment is limited to looking for evidence of the specific crimes that the police had probable cause to believe the defendant committed."). Such limitations mitigated "any possible overreach of the warrant" and required the executing officers to restrict their search for only evidence relating to child pornography. See United States v. Morgan, 562 F. App'x 123, 128 (3d Cir. 2014) (upholding search warrant that authorized search for specified items on all computers in the defendant's home, including hardware, software, and storage media, because child pornography images and communications can be saved under file names and formats that conceal the contents, and the search warrant specified that the search was limited to particular items that could provide evidence of the crimes for which probable cause

was established); United States v. Willard, No. 18-cr-172, 2022 WL 1136688, at *8 (E.D. Pa. Apr. 18, 2022) ("[A]ny possible overreach of the warrant was mitigated when Detective DiLuzio averred in three separate places in his probable-cause affidavit that the items that were the subject of the search 'are seized as is outlined in the affidavit of this search warrant and incorporated hereto by reference,' as pertaining solely to the charge of child pornography under 18 Cons. Stat. § 6312."); United States v. Winther, No. 11-cr-212, 2011 WL 5837083, at *8 (E.D. Pa. Nov. 18, 2011) (finding search warrant appropriate where defendant was charged with child pornography crimes, warrant permitted search of various hardware and software, and warrant limited search's scope to the offenses charged); see also United States v. Lucidonio, No. 20-cr-211, 2022 WL 7899164, at *10 (E.D. Pa. Mar. 15, 2022) ("So long as the actual search is confined to the *narrower* scope of the affidavit to 'cure' the warrant, or at least have treated excessive elements of the warrant as harmless surplusage." (quotations omitted)).

Third, the affidavit of probable cause—which was explicitly incorporated as part of the search warrant and numbered as pages four to twenty-six of a twenty-six page packet—recounted the eight-month investigation of Defendant's activities, identified the federal criminal statutes that Defendant allegedly violated, described the characteristics of a child pornography collector, explained the computer technology used and how such technology is utilized in both manufacture and receipt of child pornography, gave background on Twitch Interactive, and connected Defendant's computer usage with his residence. The basis for the seizure of each of the items listed in the actual application was set forth in extensive detail throughout the affidavit, and it explained precisely why all electronic storage devices must be seized in such a situation. (Affidavit of Prob. Cause ¶ 8.) Based on these averments, the magistrate could properly conclude that there was a fair probability that a full search of Defendant's computer and digital devices would uncover evidence of child pornography. Willard, 2022 WL 1136688, at *7–8.

Finally, to the extent Defendant contends that the Government had additional information available to make the search of the items seized more particular, Defendant fails to detail precisely what

additional information was available. Defendant argues that the Government could have, for example, "provided more particularity by using common search limitations like specific software used to download or store child pornography." (Def.'s Mot. 10.) As noted by the Government, however, the affidavit explained that Defendant was not suspected of downloading child pornography from the internet, meaning that there was no "specific software" or "common search limitations used." Rather, Defendant was believed to be contacting and targeting minors using the Twitch gaming app, and then enticing them to manufacture the child pornography. Moreover, as set forth in the affidavit, Twitch can be streamed from almost any platform capable of viewing videos, meaning that a more expansive search of the seized devices was justified. Finally, according to the investigation, Defendant used proxy servers to mask his IP address, thus requiring investigators to broadly search IP addresses connected to his residence.

Given all of the above, I find that the warrant adequately satisfied the Fourth Amendment's particularity requirement. The warrant limited the search to certain types of documents, computer hardware, and computer software that had a direct connection to the types of crimes being committed, and it confined the discretion of the executing agents to relevant evidence. Accordingly, I find that the search warrant was supported by probable cause, and, as such, no basis exists to suppress the recovered evidence.[2]

B. Whether Defendant's Statements Must Be Suppressed

Also at issue are two inculpatory statements given by Defendant to law enforcement. The first was given at his home, before he was in custody, at the time of the execution of the search warrant. The second occurred while he was in custody at the Delaware County Criminal Investigation Division, awaiting his initial court appearances.

[2] Defendant also addresses whether the good faith exception applies. As I find that the search warrant was proper, I need not address this argument.

Defendant argues that he only made incriminatory statements to officers because the officers informed him about the search of his residence. Defendant does not challenge the voluntariness of either statement, nor does he allege that he was not properly and timely advised of his Miranda rights. Rather, he contends that because the search of his residence was unconstitutional, his statements are fruits of an illegal search and must be suppressed under the "fruit of the poisonous tree" doctrine. Segura v. United States, 468 U.S. 796, 804 (1984) (noting that "the exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, . . . but also evidence later discovered and found to be derivative of an illegality or 'fruit of the poisonous tree.'" (internal citations and quotations omitted).)

As I have found that the search warrant is valid and, in turn, that the search of Defendant's home was lawful, I have no basis on which to suppress the statements as fruit of the poisonous tree. Accordingly, I will deny this portion of the motion to suppress as well.

An appropriate Order follows.